SPF Compliance Checklist

SPF Security Compliance

This compliance checklist is designed to assist businesses, agencies or other organisations, in assessing their ability to meet the requirements of the UK Government's Security Policy Framework. It is not a substitute for a detailed assessment by a professional and is not suitable for submission to HMG agencies as proof of compliance. This is provided "as is" without any warranty or guarantees. It is essential that current regulations are checked to properly determine compliance.

Security Risk Management

Security Policy Framework Compliance

Audit Checklist

SPF Version 7.0 (October 2011)

Checklist Version 2.0 (November 2011)

Security Policy Framework (v 7.0) Audit Check List

Auditor Name: ..... Audit Date: .....

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
Governance and Security Approaches					
1.1		Roles, Accountability and Responsibilities			
1.1.1	1		Identify board level representative responsible for security		
1.1.2	1		Identify designated SIRO		
1.1.3	1		Ensure SIRO responsibilities include management of organisation's information risks.		
1.1.4	1		Ensure the Information Risk Register is properly maintained.		
1.1.5	1		Identify designated DSO.		

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
1.1.6	1		Ensure DSO day to day responsibilities cover all aspects of Protective Security		
1.1.7	1		Review requirements for specialist security roles.		
1.1.8	1		Review documentation detailing security responsibilities.		
1.1.9	1		Ensure all individuals with designated security responsibilities have appropriate training for the role.		
1.2		Security Risk Management			
1.2.1	2		Adopt an organisation-wide holistic risk management approach to protective security which is aligned to HMT Orange Book principles.		
1.2.2	2		Develop local security policies tailored to relevant business needs, threat profiles and risk appetite.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
1.2.3	2		Maintain a Protective Security Risk Register		
1.3		Culture, Education and Awareness			
1.3.1	3		Ensure all staff are provided with guidance regarding relevant legislation (OSA, DPA, FOIA etc).		
1.3.2	3		Ensure staff handling PMM are given specific guidance on how legislation relates to their role.		
1.3.3	3		Ensure Security awareness & education is built into staff induction.		
1.3.4	3		Ensure all staff complete regular security familiarisation.		
1.3.5	3		Ensure there are demonstrable plans to foster a culture of proportionate protective security.		
1.3.6	3		Ensure all users of ICT systems are familiar with SyOPS and have received appropriate		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			security training for their use.		
1.3.7	3		Ensure there is a clearly stated and available policy, with supporting mechanisms, to allow for independent and anonymous reporting of security incidents.		
1.4		Managing and Recovering from Incidents			
1.4.1	4		Ensure there is an effective and up-to-date Business Continuity Management (BCM) system.		
1.4.2	4		Provide evidence that BCM arrangements follow best practice (BS25999 or equivalent).		
1.4.3	4		Ensure that BCM strategy is endorsed by Board-level management and reviewed by competent & well trained staff.		
1.4.4	4		Ensure there is an effective system for detecting, reporting and responding to security breaches including incident management structures, investigation		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			capability and escalation procedures.		
1.5		Assurance and Reporting			
1.5.1	5		Ensure systems in place to provide assurance that organisation (and delivery partners / 3rd party suppliers) comply with security policy requirements.		
1.5.2	5		Produce annual report to HoD on the state of protective security and information risk including an explicit statement of assurance on Counter Terrorist protective security.		
1.5.3	5		Provide reporting to HoD regarding additional protective measures implemented following any increase in the Government Response Level, and any testing.		
1.5.4	5		Reflect any significant identified control weaknesses in the Governance Statement to the annual Resource Accounts.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
1.5.5	5		Submit or contribute to an annual Cabinet Office Security Risk Management overview.		
Security of Information					
2.1		Information Security Policy			
2.1.1	6		Ensure information security roles have been properly identified and aligned to business functions / structures.		
2.1.2.	6		Review policies, procedures and controls to ensure compliance with legal requirements and the standards set out in GPMS and supporting CESG Technical and IA Standards.		
2.1.3	6		Verify policies, procedures and controls are widely adopted across the organisation and properly implemented.		
2.1.4	6		Organisation must ensure that non-HMG material which is marked to indicate sensitivity is handled at the equivalent		

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			level with the PM System.		
2.1.5	6		Ensure risks related to digital continuity and records management are properly managed and documented.		
2.1.6	6		Provide evidence that security and business risks relating to outsources / offshored information and / or services have been assessed and managed.		
2.2		Valuing and Classifying Assets			
2.2.1	7		Ensure information and other assets are valued in accordance with Annex One to the SPF and conspicuously marked where appropriate.		
2.2.2	7		Ensure assets are protected in accordance with the GPMS requirements.		
2.2.3	7		Ensure access to sensitive assets and information is only granted on a “need to know” basis and subject to an appropriate level of personnel security control.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.2.4	7		Ensure that when information is shared for business purposes, that the receiving party understands the obligations and protects the assets appropriately.		
2.2.5	7		Assets sent overseas (including to UK posts) must be protected as indicated by the originators marking.		
2.2.6	7		Assets sent overseas (including to UK posts) are protected from foreign FOI legislation as required.		
2.2.7	7		Ensure all staff handling sensitive government assets are briefed about how legislation (particularly the OSA, FOIA and DPA) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies.		
2.2.8	7		Ensure appropriate management structures must be in place to ensure the proper handling, control and (if		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			appropriate) managed disclosure of sensitive assets.		
2.3		Risk Assessment and Accreditation of ICT systems			
2.3.1	8		Conduct technical risk assessments for all ICT systems or services (recorded in RMADS).		
2.3.2	8		Ensure technical risk assessments are repeated annually or whenever there are significant changes to a risk component (threat, vulnerability, business use, impact etc)		
2.3.3	8		Where personal data is processed ensure all handling and protection is compliant with the requirements of HMG IA Standard 6.		
2.3.4	8		Ensure there is the ability to audit information assets and ICT systems to check compliance and extract data in the event of an incident.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.3.5	8		Where shared systems or services are used, an assessment must be made to confirm that use of these systems or services can be managed within the appropriate risk appetite.		
2.4		Risk Treatment – Technical, Procedural and Physical Security Controls			
2.4.1		Technical Controls			
2.4.1.1	9		Ensure compliance with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories.		
2.4.1.2	9		Put in place a proportionate risk based suite of technical policies and controls covering: Patching Boundary Protection Content Checking / Blocking		

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			Protective Monitoring Lockdown of unnecessary services User account management		
2.4.1.3	9		Ensure that action is taken to develop and keep up to date an appropriate understanding of new, emerging and changing threats and vulnerabilities		
2.4.1.4	9		Comply with the requirements of "HMG IA Standard No.4 - Communications Security and Cryptography" for the protection of any cryptographic items.		
2.4.1.5	9		Organisations that handle CESG approved cryptographic material must appoint a Communications Security Officer (ComSo).		
2.4.1.6	9		Where applicable, comply with mandated Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations		
2.4.1.7	9		Ensure that all portable devices and media		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			used for mobile or remote working are appropriately secured.		
2.4.1.8	9		For online services, keep abreast of and respond to changing threat conditions.		
2.4.1.9	9		Have a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system that may be required for legal and management purposes.		
2.4.1.10	9		Ensure that all media used for storing or processing protectively marked information is disposed of, or sanitised, in accordance with "HMG IA Standard No 5 - Secure Sanitisation."		
2.4.2		Procedural Measures			
2.4.2.1	10		Implement appropriate identification and authentication controls, policies and procedures to manage the risk of unauthorised access, ensure the correct management of user accounts and enable		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			auditing.		
2.4.2.2	10		Ensure that ICT users with higher levels of privilege and/or potentially wide access, or those with responsibilities for ICT security are evaluated for National Security clearances as appropriate.		
2.4.2.3	10		Ensure that all users of ICT systems comply with the security operating procedures governing their use, receive appropriate security training, and are aware of local processes for reporting issues of security concern.		
2.4.2.4	10		Put in place appropriate policies and procedures to support mobile and remote working and ensure users are briefed on, and accept, their security responsibilities.		
2.4.3		Delivery Partners and Third Party Suppliers			
2.4.3.1	11		Ensure assurance is provided from delivery partners that they are managing their protective security and information risks to		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			an appropriate level.		
2.4.3.2	11		Document how procurement and contract management teams work with security to ensure that adequate provisions are put in place.		
2.4.3.3	11		Ensure all contracts involving the handling of personal data adhere to OGC model terms and conditions.		
2.4.3.4	11		Comply with HMG requirements and procedures governing the off-shoring of data.		
2.4.3.5	11		Put in place appropriate governance arrangements to annually review the compliance of delivery partners and third party suppliers against the Security Policy Framework. (This must be managed independently of the organisation providing the service)		
2.5		Managing and Reporting Security Incidents			

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.5.1	12		Ensure there is a security incident policy which establishes clear guidance for staff on the potential disciplinary and / or criminal penalties that may result from failure to comply with security policies.		
2.5.2	12		Ensure that all staff are informed of their responsibilities to report incidents promptly.		
2.5.3	12		Establish, and document, appropriate management structures to co-ordinate the organisations response to information security incidents.		
2.5.4	12		Ensure all staff are aware of the procedures for reporting incidents.		
2.5.6	12		Ensure that ICT systems and information assets maintain sufficient data to support post incident investigations.		
2.5.7	12		Ensure that incident management procedures provide sufficient data collection to support post incident		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			investigations.		
2.5.8	12		Ensure incidents are reported to the relevant central authority.		
Personnel Security					
3.1		Recruitment Checks and National Security Vetting			
3.1.1	13		Ensure that the Baseline Personnel Security Standard (BPSS) is applied to all individuals employed by or contracted to carry out work for any government department. In any instances where this is not possible (e.g. some overseas recruits), the decision to accept the risk should be recorded.		
3.1.2	13		Determine the need for, and level of, national security vetting clearance required to fulfil the duties of the post based on a thorough risk assessment.		
3.1.3	13		Apply national security vetting in accordance with the HMG Statement of Vetting Policy, as transparently as any		

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			national security considerations allow.		
3.1.4	13		Record and maintain a register of appropriate decisions.		
3.2		Ongoing Personnel Security Management			
3.2.1	14		Keep full and up to date personnel security records on all employees that hold security clearances.		
3.2.2	14		Ensure that movement, or loans, of staff do not commence until the receiving organisation has confirmation of the appropriate security clearance and of any caveats that have been applied.		
3.2.3	14		Ensure that NSV clearances are formally reviewed according to agreed timescales for each level of clearance.		
3.2.4	14		Ensure than an Annual Security Appraisal Form (SAF) is completed by all DV holders and, in those instances where is applicable, SC and CTC holders.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
3.2.5	14		Establish a programme of management where risks or vulnerabilities have been identified.		
3.2.6	14		Ensure that any new information or concerns that may affect the reliability of an individual are reported to the appropriate authorities.		
3.3		Appeals			
3.3.1	15		Ensure that the reasons for refusing an existing employee a national security vetting clearance are recorded in full and that the individual is informed, subject to national security considerations, of the reasons for the refusal with reference to the relevant facts		
3.3.2	15		Ensure that the employee is informed, fully and clearly, of the mechanisms for internal and external appeal and that any factual information that can be shared is shared with the individual.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
3.3.3	15		Provide an agreed factual account of any interview proceedings that gave rise to concerns and ensure that third party information provided in confidence, or information supplied by the Security Service, is not shared with the individual.		
3.3.4	15		Establish a clear policy on redeploying individuals that have been refused a clearance in areas where identified risks can be managed.		
3.3.5	15		Ensure the policy outlines dismissal procedures and handling those instances where it is not possible to continue to employ the individual because of security objections.		
Physical Security and Counter Terrorism					
4.1		Security Risk Assessment			
4.1.1	16		Ensure physical security risks are managed in accordance with the requirements set		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			out in Security Policy No. 1: Governance and Security Approaches (MR2), in line with the organisation's overall risk tolerance		
4.1.2	16		Ensure a record is kept of the value of assets, their location and the impact of compromise or loss, both of the assets themselves and any key locations.		
4.1.3	16		Assess and document the level of threat to assets from different sources (including terrorism, espionage, criminal activity, protests etc), including the vulnerability of sites to threats and hazards identified in the National Risk Assessment or National Risk Register.		
4.1.4	16		Categorise all establishments (HIGH, MODERATE, and LOW) according to the likelihood of being the target of a terrorist attack, or else in close proximity to an attack.		

Security Policy Framework (v 7.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.1.5	16		Undertake regular security risk assessments for all establishments in their estate (and any non-government sites that sustain core business, such as data centres), using approved methodologies and approaches, where appropriate, commercial best practice equivalents		
4.1.6	16		Ensure that a detailed Operational Requirement is produced to inform any decision about purchasing or deploying a new security system or product.		
4.2		Internal Controls			
4.2.1	17		Ensure that sensitive or valuable assets (including paper-based assets, ICT hardware and removable media devices) are physically protected to the standards required by the Government Protective Marking System, including through the use of appropriate security furniture, secure areas, barriers and entry controls (in conjunction with sound procedural and		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			personnel security controls).		
4.2.2	17		Ensure that any security furniture, windows, doors, locks, barriers and entry controls meet appropriate security standards for the protection of sensitive or protectively marked assets.		
4.2.3	17		Put in place and enforce appropriate policies to ensure that visitors, cleaners and maintenance workers are escorted at all times in sensitive areas. This requirement may be risk managed where individuals hold an appropriate level of security clearance.		
4.2.4	17		Access control and breach management policies must be made available to all staff, and staff must be briefed on their personal responsibilities.		
4.2.5	17		Adopt „clear desk" and „clear screen" policies in areas where sensitive assets are handled (particularly in open plan or		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			shared office areas).		
4.2.6	17		Ensure that computer screens, faxes, printers, combination locks and office areas that are used to display potentially sensitive information are sited or screened such that they cannot be overlooked by unauthorised individuals, inside or outside the building.		
4.2.7	17		Carry out, and maintain a record of, compliance checking activities to ensure the effectiveness of physical security control measures.		
4.3		Building and Perimeter Security			
4.3.1	18		Establish a secure boundary or perimeter through appropriate use of security barriers and entry controls.		
4.3.2	18		Ensure that the external fabric of buildings (external walls, windows, doors etc.) is suitably robust to provide an appropriate level of blast protection and resistance to		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			forced or surreptitious attack.		
4.3.3	18		Ensure arrangements are in place to control and manage access to the estate.		
4.3.4	18		Ensure frontline staff are supported by appropriate technical and procedural controls.		
4.3.5	18		Ensure buildings containing protectively marked, or other valuable assets have as few entry and exit points as business functions and safety will allow.		
4.3.6	18		Ensure effective plans or procedures are in place for dealing with and intercepting unauthorised visitors, intruders or suspicious items.		
4.3.7	18		Document assessment over the use of manned guard forces to deter hostile activity, including reasons for or against any deployment.		
4.3.8	18		Ensure procedures are in place to screen		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			incoming mail and deliveries for suspicious items.		
4.4		Preparing for Critical Incidents			
4.4.1	19		Ensure baseline CT requirements are implemented.		
4.4.2	19		Identify an appropriate and proportionate range of incremental measures for each site that can be applied immediately in response to any increase in the Government Response Level.		
4.4.3	19		Develop appropriate Counter-Terrorist contingency arrangements and plans (as part of wider Business Continuity Planning) setting out the procedures to be followed in the event of an incident or imminent terrorist threat.		
4.4.4	19		Test, and record outcomes, all CT arrangements and contingency plans and take action to correct any identified issues.		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.4.5	19		Report the results of any tests of CT arrangements in the Annual Report to the Head of Department, and report any issues or lessons learned to the Cabinet Office in the annual Security Risk Management Overview.		
4.5		Responding to Critical Incidents			
4.5.1	20		Document, and test, a process for immediately imposing a pre-determined set of additional physical security controls following any increase in the Government Response Level.		
4.5.2	20		Ensure that appropriate and resilient arrangements are in place for the management of any critical incident, including assigned roles and responsibilities and effective decision-making channels.		
4.5.3	20		Document, and test, a strategy for communicating with staff, emergency		

Security Policy Framework (v 7.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			responders and the media (also including consideration of handling enquiries from concerned family and friends).		
4.5.4	20		Document, and test, search plans for each establishment and plans for responding to incidents out of regular hours, as appropriate.		
4.5.5	20		Report to the Head of Department summarising steps taken and additional controls implemented following any change to the Government Response Level. Any issues or lessons learned should be reported to the Cabinet Office in the annual Security Risk Management Overview.		

Halkyn Security Consulting Ltd

Halkyn Security is an independent security consultancy offering a specialised security compliance service to assist enterprises of all sizes become compliant with HMG regulations, and remain compliant for the lifetime of contracts. As an independent consultancy all our security advice is vendor neutral and we are committed to ensuring our clients get the best possible value for money.

We utilise experienced staff with a minimum of SC clearance to conduct detailed assessments against current regulations to allow you, or your key stakeholders, to determine what your current security posture is and what (if anything) would be required to meet the standards laid down by the relevant Government Department or Agency.

For companies currently working on Government contracts we offer a review service to ensure that you are still current with the regulations and that you have employed the most cost effective solutions. While this is not in place of the reviews carried out by the sponsoring Agency, it will place you in the best possible position to ensure a clean bill of health.

To find out more, or get a free, no-obligation quote visit **www.halkynconsulting.co.uk** or email **info@halkynconsulting.co.uk** with your requirements.